

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-112804

(43)Date of publication of application : 21.04.2000

(51)Int.Cl.

G06F 12/00

(21)Application number : 10-279918

(71)Applicant : NEC CORP

(22)Date of filing : 01.10.1998

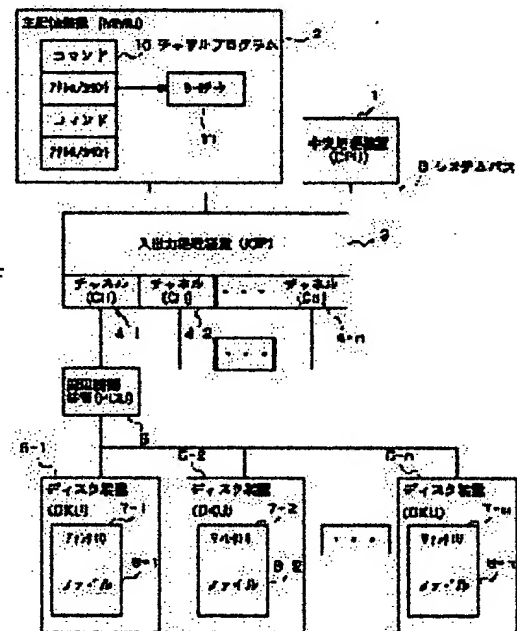
(72)Inventor : IIDA SHOZO

(54) METHOD FOR PROTECTING FILE AND VIRTUAL COMPUTER SYSTEM BY THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an operating system(OS) from accessing the data file of another OS in a virtual computer system.

SOLUTION: This is a file protection method in a virtual computer system in which plural OSs operate by sharing plural files on one computer. In this case, an OS capable of accessing each of files 81 to 8n is set up and an access to the file is permitted only for the OS capable of accessing the file.



LEGAL STATUS

[Date of request for examination]

01.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-112804

(P2000-112804A)

(43) 公開日 平成12年4月21日 (2000. 4. 21)

(51) Int.Cl.⁷

G 0 6 F 12/00

識別記号

5 3 5

F I

G 0 6 F 12/00

テーマコード(参考)

5 3 5 A 5 B 0 8 2

審査請求 有 請求項の数 6 O L (全 6 頁)

(21) 出願番号 特願平10-279918

(22) 出願日 平成10年10月1日 (1998. 10. 1)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 飯田 昌三

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100100893

弁理士 渡辺 勝 (外3名)

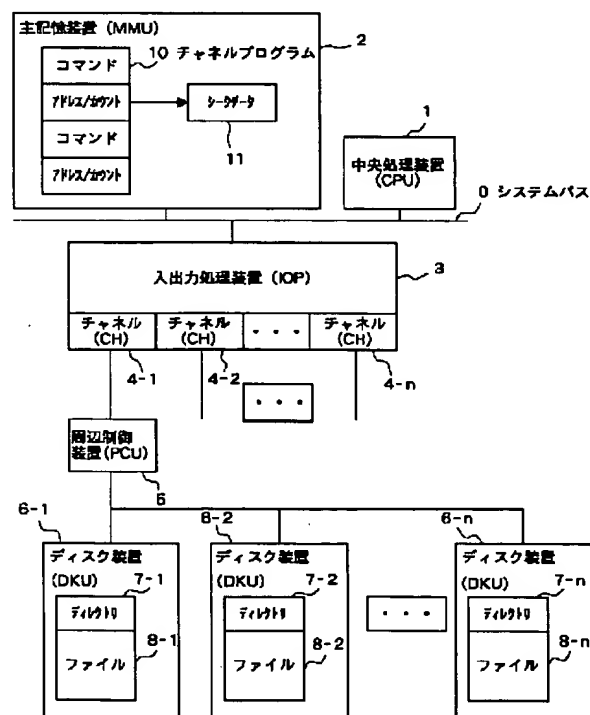
Fターム(参考) 5B082 EA07 FA16

(54) 【発明の名称】 ファイル保護方法およびこれによる仮想計算機システム

(57) 【要約】

【課題】 仮想計算機システムにおいて、OSが、他のOSのデータファイルにアクセスすることを防止する。

【解決手段】 複数のオペレーティングシステムが1つの計算機上で複数のファイルを共用して動作する仮想計算機システムにおけるファイル保護方法であって、各ファイルについて、当該ファイルにアクセス可能なオペレーティングシステムを設定し、アクセス可能とされたオペレーティングシステムのみアクセスを許可する。



【特許請求の範囲】

【請求項 1】 複数のオペレーティングシステムが 1 つの計算機上で複数のファイルを共用して動作する仮想計算機システムにおけるファイル保護方法であって、各ファイルについて、当該ファイルにアクセス可能なオペレーティングシステムを設定し、アクセス可能とされたオペレーティングシステムのみにアクセスを許可することを特徴とするファイル保護方法。

【請求項 2】 複数のオペレーティングシステムが 1 つの計算機上で複数のファイルを共用して動作する仮想計算機システムにおけるファイル保護方法であって、各ファイルについて、当該ファイルにアクセス可能なオペレーティングシステムを示す OS 番号を設定し、オペレーティングシステムがファイルをアクセスする要求を含む命令を出力した場合には、要求を出したオペレーティングシステムを示す OS 番号を命令に付与し、ファイルに設定された OS 番号と命令に付与された OS 番号が一致した場合にのみファイルへのアクセスを許可することを特徴とするファイル保護方法。

【請求項 3】 中央処理装置と、複数のオペレーティングシステムやアプリケーションプログラムを格納する主記憶装置と、それぞれファイルを格納する複数のディスク装置とを具備し、複数のオペレーティングシステムが複数のファイルを共用して動作する仮想計算機システムであって、前記複数のディスク装置に格納される各ファイルには当該ファイルにアクセス可能なオペレーティングシステムを示す OS 番号が設定されており、前記中央処理装置は、所定のオペレーティングシステムからの所定のファイルをアクセスする要求を含む I/O 命令を検出すると、前記入出力処理装置にプログラムを実行するための入出力を定義するとともに所定のオペレーティングシステムを示す OS 番号が付与された I/O 制御語を送出し、所定のファイルを格納するディスク装置は、当該ファイルに設定された OS 番号と前記 I/O 制御語に付与された OS 番号が一致した場合にのみ前記 I/O 命令に則った処理を続行することを特徴とする仮想計算機システム。

【請求項 4】 請求項 3 記載の仮想計算機システムにおいて、ディスク装置は、当該ファイルに設定された OS 番号と前記 I/O 制御語に付与された OS 番号が一致しない場合にはエラーステータスを中央処理装置へ出力することを特徴とする仮想計算機システム。

【請求項 5】 請求項 3 または請求項 4 に記載の仮想計算機システムにおいて、中央処理装置および主記憶装置とシステムバスを介して接続された複数のチャンネルを収容する入出力処理装置を具備し、ディスク装置は該入出力装置に収容された所定

のチャンネルを介して前記 I/O 制御語に付与された OS 番号を受け取ることを特徴とする仮想計算機システム。

【請求項 6】 請求項 5 記載の仮想計算機システムにおいて、

複数のチャンネルと複数のディスク装置との間に設けられた周辺制御装置をさらに具備し、ディスク装置は該周辺制御装置を介して前記 I/O 制御語に付与された OS 番号を受け取ることを特徴とする仮想計算機システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、複数のオペレーティングシステム（以下、OS と称する）が 1 つの計算機上で動作する仮想計算機システムでのファイル保護方法およびこれによる仮想計算機システムに関する。

【0002】

【従来の技術】 ファイル保護方式はファイルの誤用、誤修正、及びアクセスすることができる人が限定されている特定のファイルを他人がアクセスすることを防ぐために行われる。従来のファイル保護方式では、個々のファイルを他のファイルと識別するための記号、ラベル等を各ファイルに付け、記号やラベルに応じたアクセス規制を設けることにより、特定ファイル、または、その一部に誤った処理、修正が行われることを防いでいた。

【0003】

【発明が解決しようとする課題】 しかしながら、従来のファイル保護方式においては、次のような課題がある。1 つのシステム上で複数の OS がファイルを共用して動作する仮想計算機システムでは、各 OS が 1 つの記憶装置（ディスク）を共用する場合、各 OS は個別にディスク内のファイルに記号やラベルを付けることができる。そのため、各 OS が誤って互いに同じ記号やラベルを持つ、同じサイズのファイルを、同じディスクの、同じアドレスに格納しようとした場合に生じるファイル破壊を防ぐことができない。

【0004】 本発明は、上述したような従来の技術が有する問題点を鑑みてなされたものであって、1 つのシステム上で複数の OS がファイルを共用して動作する仮想計算機システムにおいて、OS が、他の OS のデータファイルをアクセスすることを防止することのできるファイル保護方法およびこれによる仮想計算機システムを実現することを目的とする。

【0005】

【課題を解決するための手段】 本発明のファイル保護方法は、複数のオペレーティングシステムが 1 つの計算機上で複数のファイルを共用して動作する仮想計算機システムにおけるファイル保護方法であって、各ファイルについて、当該ファイルにアクセス可能なオペレーティングシステムを設定し、アクセス可能とされたオペレーティングシステムのみにアクセスを許可することを特徴とする。

【0006】本発明の他の形態によるファイル保護方法は、複数のオペレーティングシステムが1つの計算機上で複数のファイルを共用して動作する仮想計算機システムにおけるファイル保護方法であって、各ファイルについて、当該ファイルにアクセス可能なオペレーティングシステムを示すOS番号を設定し、オペレーティングシステムがファイルをアクセスする要求を含む命令を出力した場合には、要求を出したオペレーティングシステムを示すOS番号を命令に付与し、ファイルに設定されたOS番号と命令に付与されたOS番号が一致した場合にのみファイルへのアクセスを許可することの特徴とする。

【0007】本発明の仮想計算機システムは、中央処理装置と、複数のオペレーティングシステムやアプリケーションプログラムを格納する主記憶装置と、それぞれファイルを格納する複数のディスク装置とを具備し、複数のオペレーティングシステムが複数のファイルを共用して動作する仮想計算機システムであって、前記複数のディスク装置に格納される各ファイルには当該ファイルにアクセス可能なオペレーティングシステムを示すOS番号が設定されており、前記中央処理装置は、所定のオペレーティングシステムからの所定のファイルをアクセスする要求を含むI/O命令を検出すると、前記入出力処理装置にプログラムを実行するための入出力を定義するとともに所定のオペレーティングシステムを示すOS番号が付与されたI/O制御語を送出し、所定のファイルを格納するディスク装置は、当該ファイルに設定されたOS番号と前記I/O制御語に付与されたOS番号が一致した場合にのみ前記I/O命令に則った処理を続行することを特徴とする。

【0008】この場合、ディスク装置は、当該ファイルに設定されたOS番号と前記I/O制御語に付与されたOS番号が一致しない場合にはエラーステータスを中央処理装置へ出力することとしてもよい。

【0009】また、中央処理装置および主記憶装置とシステムバスを介して接続された複数のチャンネルを収容する入出力処理装置を具備し、ディスク装置は該入出力装置に収容された所定のチャンネルを介して前記I/O制御語に付与されたOS番号を受け取ることとしてもよい。

【0010】さらに、複数のチャンネルと複数のディスク装置との間に設けられた周辺制御装置をさらに具備し、ディスク装置は該周辺制御装置を介して前記I/O制御語に付与されたOS番号を受け取ることとしてもよい。

【0011】「作用」本発明は、OSが周辺装置のファイルをアクセスするとき、周辺装置がアクセス要求元のOSとファイルが属するOS番号が一致したときのみアクセスを許可し、不一致を検出してCPUにエラーが通知されるので、他のOSで使用されるファイルが誤ってアクセスされることがない。

【0012】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。

【0013】図1は本発明によるファイル保護方式を実現するためのシステムの一実施例の構成を示すブロック図である。

【0014】本実施例は、システムバス0と、中央処理装置(CPU)1と、複数のOSやアプリケーションプログラムを格納する主記憶装置(MMU)2と、入出力処理装置(IOP)3と、入出力処理装置3に収容される複数のチャンネル4-1~4-nと、周辺制御装置(PCU)5と、複数のディスク装置6-1~6-nから構成されている。複数のディスク装置6-1~6-nの各ディレクトリ7-1~7-nにはファイル8-1~8-nが格納されている。

【0015】中央処理装置1はシステムバス0を介して主記憶装置2と入出力処理装置3に接続され、主記憶装置2に格納されているOSやアプリケーションプログラムを実行する。

【0016】主記憶装置2は、入出力(I/O)命令を検出したときに、これに応じてチャンネルプログラム、本実施例においては、チャンネルプログラム10を用意し、入出力処理装置3にI/O処理を行うためのI/O制御語を送出する。

【0017】入出力処理装置3はチャンネルプログラム10を実行して主記憶装置2と周辺制御装置5との間の入出力処理を行う。

【0018】周辺制御装置5は、複数のチャンネル4-1~4-nのうちのいずれかと複数のディスク装置6-1~6-nとの間に設けられ、コマンド実行及びデータ転送制御を行う。

【0019】上記のチャンネルプログラム10はコマンド形式、シークデータ形式で記述されたプログラムから構成されている。図2は本実施例で用いられる各データの構造を示す図である。図2(a)、(b)はチャンネルプログラム10を構成するコマンド形式12およびシークデータ形式13の構造を示し、図2(c)は、各ディスク装置6-1~6-nの各ディレクトリ7-1~7-nを示すデータ14の構造を示し、図2(d)は主記憶装置2から入出力処理装置3に出力されるI/O制御語15の形式を示す図である。

【0020】コマンド形式12はコマンドの種類、デバイスの番号、アクセスエラー(AE)、フラグ、チャンネルに対して実行すべき操作を指定するチャンネル命令、レコード番号を示すデータから構成されており、これに対応するシークデータ形式13はアドレスおよび転送すべきバイト数を示すカウントから構成されている。図1に示す実施例ではコマンド形式12およびシークデータ形式によりシークデータ11が読み出された状態が示されている。

【0021】各ディレクトリのデータ14は、各ディレ

ディレクトリのアドレスおよびカウントと、これに対応して付されたOS番号、図示する例ではVMID#から構成されている。I/O制御語15は、コネクティブ、A/E、OS番号、チャンネル番号およびアドレッシングモードから構成されている。

【0022】上記のOS番号は複数のOSを示すもので、本実施例においてはディレクトリのデータ14およびI/O制御語15にOS番号を付されている。ディレクトリのデータ14はファイルにアクセス可能なOSを示し、I/O制御語に付されるOS番号はI/O命令を発生したOSを示すもので、これらが一致したときのみファイルへのアクセスが許可される。

【0023】複数のディスク装置6-1～6-nのそれぞれは、複数のファイル8-1～8-nのうちのシークデータ11が指示するファイル8にアクセスするとき、アクセス要求元のOSとファイル8に対応するディレクトリのOS番号の不一致を検出すると、そのOSにエラーステータスを通知してI/O処理を終了させる。図3は本実施例の動作を示すフローチャートであり、以下に図3を参照して本実施例の動作を説明する。

【0024】中央処理装置1上では複数のOSとアプリケーションプログラムが動作する。中央処理装置1が所定のOSからのI/O命令を検出すると（ステップS1）、主記憶装置2に該I/O命令に応じたチャンネルプログラム10を用意し（ステップS2）、入出力処理装置3にI/O制御語15を送出する（ステップS3）。入出力処理装置3はI/O制御語15に含まれるチャンネル番号に対応するチャンネル（例えば4-1）に接続された周辺制御装置5に対してI/O要求があることを通知する（ステップS4）。

【0025】I/O要求を受け付けた周辺制御装置5は、チャンネル（4-1）経由で入出力処理装置3にコマンド送付を要求する（ステップS5）。

【0026】入出力処理装置3はチャンネルプログラム10からコマンドを読み出し、I/O制御語15内のOS番号を付加して周辺制御装置5に送る（ステップS6）。

【0027】周辺制御装置5はコマンドを解釈し、入出力処理装置3にシークデータを要求する（ステップS7）。

【0028】入出力処理装置3はチャンネルプログラム10のアドレス/カウントが指示するシークデータ11を読み出し、周辺制御装置5に送る（ステップS8）。

【0029】周辺制御装置5はコマンド内のデバイス番号に対応するディスク装置（例えば6-1）にシークデータ11とOS番号を送る（ステップS9）。

【0030】ディスク装置（6-1）はディレクトリ（7-1）からシークデータ11に対応するエントリを

探す。該当するエントリがなければ新たにエントリを登録する。該当するエントリがあればシークデータ11のOS番号と比較する（ステップS10）。その後、ステップS10における比較の結果、OS番号が一致したかの確認を行い（ステップS11）、OS番号が一致した場合、ディスク装置（6-1）はI/O処理を実行し（ステップS12）、不一致の場合はエラーステータスを周辺制御装置5に返す（ステップS13）。

【0031】周辺制御装置5はそのエラーステータスをCH4、入出力処理装置3を経由して中央処理装置1に通知する。

【0032】

【発明の効果】以上説明したように、本発明においては、複数のOSが1つのシステム上で動作する環境下でディスク装置のファイルにアクセスするとき、そのファイルを作成したOS以外のOSからの要求であることを検出することにより、誤って他のOSのデータファイルにアクセスするのを防止することができる効果がある。

【図面の簡単な説明】

【図1】本発明によるファイル保護方式を実現するためのシステムの一実施例の構成を示すブロック図である。

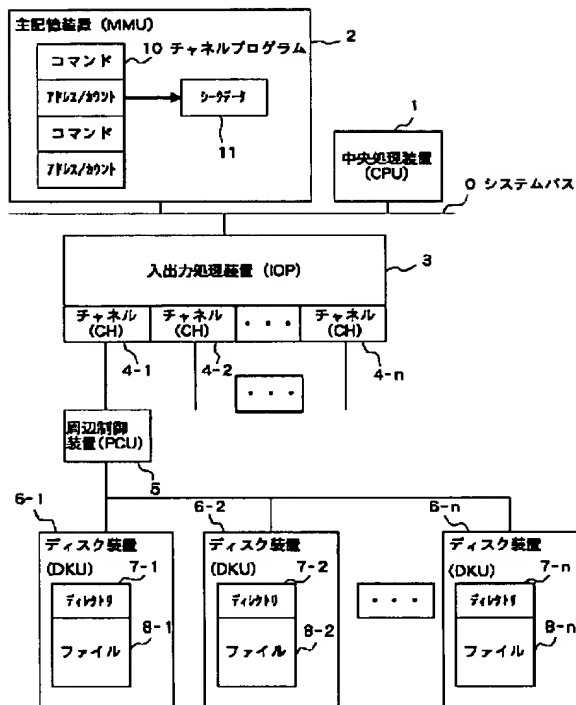
【図2】図1に示した実施例で用いられる各データの構造を示す図であり、（a）、（b）はチャンネルプログラム10を構成するコマンド形式12およびシークデータ形式13の構造を示し、（c）は、各ディスク装置6-1～6-nの各ディレクトリ7-1～7-nを示すデータ14の構造を示し、（d）は主記憶装置2から入出力処理装置3に出力されるI/O制御語15の形式を示す図である。

【図3】図1に示した実施例の動作を示すフローチャートである。

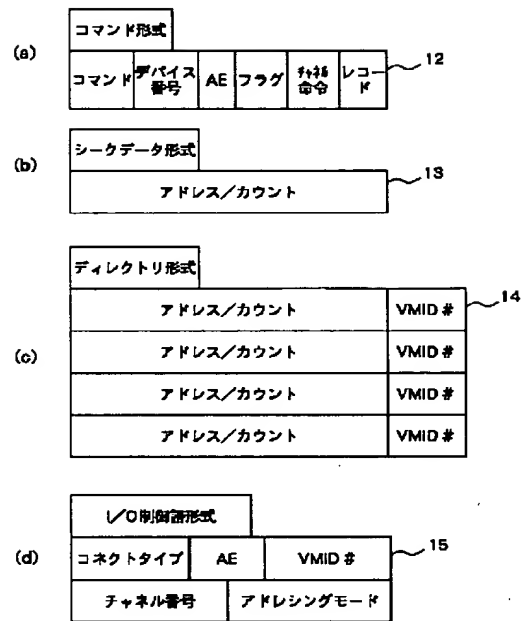
【符号の説明】

- 0 システムバス
- 1 中央処理装置
- 2 主記憶装置
- 3 入出力処理装置
- 4-1～4-n チャンネル
- 5 周辺制御装置
- 6-1～6-n ディスク装置
- 7-1～7-n ディレクトリ
- 8-1～8-n ファイル
- 10 チャンネルプログラム
- 11 シークデータ
- 12 コマンド形式
- 13 シークデータ形式
- 14 ディレクトリを示すデータ
- 15 I/O制御語

【図 1】



【図 2】



【図 3】

